Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.6 NTP-Zeitsynchronisation

1. Beschreibung

1.1. Einleitung

Vernetzte IT-Systeme erfordern oftmals synchrone Zustände. Meist dient die Uhrzeit als Referenz. Die interne Uhr von IT-Systemen kann jedoch von der tatsächlichen Zeit abweichen. Das Network Time Protocol (NTP) wird dazu verwendet, regelmäßig eine Referenzzeit zentraler Zeitgeber über Netzverbindungen zu ermitteln und die interne Uhr entsprechend anzupassen.

In Netzen erlaubt eine genaue Zeitsynchronisation Informationen mit einheitlichen Zeitstempeln zu versehen, z. B. um Daten chronologisch zu ordnen, Daten miteinander abzugleichen oder Zugriffsrechte zu befristen. Nur so lassen sich beispielsweise zeitliche Abläufe aus Protokolldaten verschiedener IT-Systeme miteinander in Beziehung bringen. Auch im Bereich der kryptographischen Protokolle sind genaue Zeitinformationen von Bedeutung. Darüber hinaus ist es in OT-Netzen essenziell, sämtliche Zeitgeber genau zu synchronisieren.

NTP-Clients beziehen Zeitinformationen von NTP-Servern. Die NTP-Server können wiederum als NTP-Clients Zeitinformationen von anderen NTP-Servern beziehen. So entsteht eine hierarchische Zeitverteilung (in sogenannte „Strata“). An der Spitze stehen NTP-Server, die ihre Zeit von genauen Quellen (z. B. einer Atomuhr, einem GPS- oder einem DCF77-Empfänger) beziehen. Diese NTP-Server werden als Stratum-1 bezeichnet.

Der NTP-Dienst nutzt Verfahren, um auch bei abweichenden Antworten verschiedener Zeitquellen die Abweichung der Systemuhr zu externen Zeitquellen zu bestimmen. Beispielsweise ignoriert er Zeitangaben einer Zeitquelle, die plötzlich gravierend von der eigenen Systemzeit abweicht.

Steuerungsnachrichten (Control Messages) erlauben es Clients, Statusinformationen abzufragen oder das Verhalten des NTP-Servers auch über das Netz hinweg zu ändern.

NTP-Nachrichten werden meistens ungesichert übertragen. NTP bietet jedoch die Möglichkeit, eine Nachricht mit kryptografischen Schlüsseln zu schützen, damit die Nachricht nicht unberechtigt verändert werden kann.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, NTP-Server und -Clients so abzusichern, dass die IT-Systeme im Informationsverbund verlässlich die Zeit ermitteln und ihre Uhren justieren können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* ist auf jedes IT-System des Informationsverbundes anzuwenden, das NTP nutzt.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- die Planung zum Einsatz des NTP-Protokolls,
- den Betrieb von NTP-Servern sowie
- den Betrieb von NTP-Clients.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Allgemeine Anforderungen an den Betrieb von Servern (siehe SYS.1.1 *Allgemeiner Server*)
- Allgemeine Anforderungen an den Betrieb von Clients (siehe SYS.2.1 *Allgemeiner Client*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* von besonderer Bedeutung.

2.1. Unzureichende Planung des Einsatzes von NTP

Unzureichende Planung kann dazu führen, dass nicht alle IT-Systeme eine ausreichend genaue Systemzeit erhalten.

Wenn nicht richtig geplant wird, wie IT-Systeme ihre Systemzeit justieren können, dann können fehlerhafte Zeitinformationen in Anwendungen entstehen. Insbesondere zeitkritische Anwendungen können in der Folge fehlerhafte Zustände aufweisen oder ausfallen.

Beispielsweise kann ein Netz so segmentiert werden, dass NTP-Server und -Clients nicht mehr miteinander kommunizieren können. Zudem kann die unzureichende Planung der Zeitsynchronisation z. B. dazu führen, dass automatisierte Prozesse zu einem falschen Zeitpunkt ausgeführt werden.

2.2. Keine oder fehlerhafte Zeitinformationen

NTP-Server können ausfallen oder falsche Zeitinformationen übermitteln.

Wenn ein IT-System seine NTP-Server nicht mehr erreichen kann, weil diese ausgefallen oder nicht erreichbar sind, dann kann es seine Systemzeit nicht mehr justieren. Dadurch kann die Zeit der internen Uhr ungenau werden.

Falls ein NTP-Server fehlerhafte Zeitinformationen an NTP-Clients übermittelt, justieren diese möglicherweise ihre Systemuhr falsch. Dadurch können fehlerhafte Zeitinformationen in Anwendungen genutzt werden, beispielsweise in Protokolldaten.

Falsche Zeitinformationen können ebenfalls dazu führen, dass zertifikatsbasierte Dienste oder Dienste, die Einmalpasswörter verwenden, nicht mehr funktionieren. Infolgedessen können sich die Benutzenden nicht mehr auf IT-Systemen oder bei Netzdiensten anmelden.

2.3. Widersprüchliche Zeitinformationen

Zeitinformationen verschiedener Quellen können sich widersprechen.

Falls ein IT-System mehrere NTP-Server verwendet, um seine Systemuhr zu justieren, dann können die Zeitinformationen der verschiedenen NTP-Server unterschiedlich sein. Sobald die Zeitinformationen untolerierbar stark voneinander abweichen, kann das IT-System möglicherweise nicht mehr bestimmen, welche der Zeitinformationen die richtige ist. Dadurch kann die Systemzeit falsch justiert werden.

2.4. Manipulation der NTP-Kommunikation

Netzpakete mit Zeitinformationen können manipuliert werden.

Das NTP-Protokoll ist für verschiedene Angriffe anfällig. Bei einem Angriff können beispielsweise die Zeitinformationen manipuliert werden, während sie übertragen werden, oder NTP-Anfragen können zu einem anderen Server umgeleitet werden. So kann bei einem Angriff die Systemzeit der NTP-Clients manipuliert werden, um beispielsweise zeitlich beschränkte Zugriffsrechte zu nutzen, obwohl sie abgelaufen sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.6 *NTP-Zeitsynchronisation* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.6.A1 Planung des NTP- Einsatzes (B)

Der IT-Betrieb MUSS planen, wo und wie NTP eingesetzt wird. Dies SOLLTE vollständig dokumentiert werden. Dabei MUSS ermittelt werden, welche Anwendungen auf eine genaue Zeitinformation angewiesen sind. Die Anforderungen des Informationsverbunds hinsichtlich genauer Zeit der IT-Systeme MÜSSEN definiert und dokumentiert werden.

Der IT-Betrieb MUSS definieren, welche NTP-Server von welchen NTP-Clients genutzt werden sollen.

Es MUSS festgelegt werden, ob NTP-Server im Client-Server- oder im Broadcast-Modus arbeiten.

OPS.1.2.6.A2 Sichere Nutzung fremder Zeitquellen (B)

Falls Zeitinformationen von einem NTP-Server außerhalb des Netzes der Institution bezogen werden, dann MUSS der IT-Betrieb beurteilen, ob der NTP-Server hinreichend verlässlich ist. Der IT-Betrieb MUSS sicherstellen, dass nur als verlässlich eingestufte NTP-Server verwendet werden. Der IT-Betrieb MUSS die Nutzungsregeln des NTP-Servers kennen und beachten.

OPS.1.2.6.A3 Sichere Konfiguration von NTP-Servern (B)

Der IT-Betrieb MUSS den NTP-Server so konfigurieren, dass Clients nur dann Einstellungen des NTP-Servers verändern können, wenn dies explizit vorgesehen ist. Darüber hinaus MUSS sichergestellt werden, dass nur vertrauenswürdige Clients Status-Informationen abfragen können.

Falls die internen NTP-Server der Institution nicht selbst hinreichend genaue Zeitquellen nutzen, dann MUSS der IT-Betrieb diese NTP-Server so konfigurieren, dass sie regelmäßig genaue Zeitinformationen von externen NTP-Servern abfragen.

OPS.1.2.6.A4 Nichtberücksichtigung unaufgeforderter Zeitinformationen (B)

Der IT-Betrieb MUSS alle NTP-Clients so konfigurieren, dass sie Zeitinformationen verwerfen, die sie unaufgefordert von anderen IT-Systemen erhalten.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.2.6.A5 Nutzung des Client-Server-Modus für NTP (S)

Der IT-Betrieb SOLLTE alle IT-Systeme so konfigurieren, dass sie den NTP-Dienst im Client-Server-Modus nutzen. NTP-Server SOLLTEN Zeitinformationen nur dann an Clients versenden, wenn diese aktiv anfragen.

OPS.1.2.6.A6 Überwachung von IT-Systemen mit NTP-Nutzung (S)

Der IT-Betrieb SOLLTE die Verfügbarkeit, die Kapazität und die Systemzeit der internen NTP-Server überwachen.

Der IT-Betrieb SOLLTE IT-Systeme, die ihre Zeit per NTP synchronisieren, so konfigurieren, dass sie folgende Ereignisse protokollieren:

- unerwartete Neustarts des IT-Systems,
- unerwartete Neustarts des NTP-Dienstes,
- Fehler im Zusammenhang mit dem NTP-Dienst sowie
- ungewöhnliche Zeitinformationen.

Falls der NTP-Server von sich aus regelmäßig Zeitinformationen versendet (Broadcast-Modus), dann SOLLTE der IT-Betrieb die NTP-Clients daraufhin überwachen, ob sie ungewöhnliche Zeitinformationen erhalten.

OPS.1.2.6.A7 Sichere Konfiguration von NTP-Clients (S)

Der IT-Betrieb SOLLTE festlegen, welche Zeitinformationen ein IT-System verwenden soll, wenn es neu gestartet wurde. Der IT-Betrieb SOLLTE festlegen, welche Zeitinformationen ein IT-System verwenden soll, wenn sein NTP-Dienst neu gestartet wurde.

Der IT-Betrieb SOLLTE festlegen, wie NTP-Clients auf stark abweichende Zeitinformationen reagieren. Insbesondere SOLLTE entschieden werden, ob stark abweichende Zeitinformationen von NTP-Servern nach einem Systemneustart akzeptiert werden. Der IT-Betrieb SOLLTE Grenzwerte für stark abweichende Zeitinformationen festlegen.

Der IT-Betrieb SOLLTE sicherstellen, dass NTP-Clients auch dann noch ausreichende Zeitinformationen erhalten, wenn sie von einem NTP-Server aufgefordert werden, weniger oder gar keine Anfragen zu senden.

OPS.1.2.6.A8 Einsatz sicherer Protokolle zur Zeitsynchronisation (S)

Der IT-Betrieb SOLLTE prüfen, ob sichere Protokolle zur Zeitsynchronisation eingesetzt werden können (z. B. Network Time Security (NTS)). Falls dies möglich ist, SOLLTEN sichere Protokolle eingesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.6.A9 Verfügbarkeit ausreichend vieler genauer Zeitquellen (H)

Falls korrekte Systemzeiten von erheblicher Bedeutung sind, dann SOLLTE eine Institution über mehrere Stratum-1-NTP-Server in ihrem Netz verfügen. Die IT-Systeme des Informationsverbunds mit NTP-Dienst SOLLTEN die Stratum-1-NTP-Server direkt oder indirekt als Zeitreferenz nutzen. Die Straum-1-Server SOLLTEN jeweils über verschiedene Zeitquellen verfügen.

OPS.1.2.6.A10 Ausschließlich interne NTP-Server (H)

Jedes IT-System des Informationsverbunds mit NTP-Dienst SOLLTE Zeitinformationen ausschließlich von NTP-Servern innerhalb des Netzes der Institution beziehen.

OPS.1.2.6.A11 Redundante NTP-Server (H)

IT-Systeme, bei denen die Genauigkeit der Systemzeit von erheblicher Bedeutung ist, SOLLTEN Zeitinformationen von mindestens vier unabhängigen NTP-Servern beziehen.

OPS.1.2.6.A12 NTP-Server mit authentifizierten Auskünften (H)

NTP-Server SOLLTEN sich bei der Kommunikation gegenüber Clients authentisieren. Dies SOLLTE auch für die Server gelten, von denen der NTP-Server seinerseits Zeitinformationen erhält. Die NTP-Clients SOLLTEN nur authentifizierte NTP-Daten akzeptieren.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.2.2 Cloud-Nutzung

1. Beschreibung

1.1. Einleitung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Cloud Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzenden abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen der Cloud-Diensteanbietenden zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben freigesetzt werden können. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht ausreichend betrachtet werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten des IT-Betriebs als auch der Benutzenden der auftraggebenden Institution, ist ein wichtiger Erfolgsfaktor.

Zusätzlich sollte bei der Einführung von Cloud-Diensten auch das Thema Governance berücksichtigt werden (Cloud Governance). Kritische Bereiche sind beispielsweise die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.

1.2. Zielsetzung

Der Baustein beschreibt Anforderungen, durch die sich Cloud-Dienste sicher nutzen lassen. Er richtet sich an alle Institutionen, die solche Dienste bereits nutzen oder sie zukünftig einsetzen wollen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.2.2 *Cloud-Nutzung* ist immer auf eine konkrete Cloud-Dienstleistung anzuwenden. Nutzt eine Institution unterschiedliche Cloud-Diensteanbietende, so ist der Baustein für alle Cloud-Diensteanbietenden anzuwenden. Die Schnittstelle zwischen den Cloud-Diensteanbietenden ist ebenfalls Gegenstand des Bausteins und muss für alle Cloud-Dienstleistungen betrachtet werden.

In nahezu allen Bereitstellungsmodellen, abgesehen von der Nutzung einer Private Cloud On-Premise, stellen Cloud-Dienste eine Sonderform des Outsourcings (siehe Baustein OPS.2.3 *Nutzung von Outsourcing*) dar. Die im vorliegenden Baustein beschriebenen Gefährdungen und Anforderungen werden daher häufig auch im Outsourcing angewendet. Bei Cloud-Diensten gibt es jedoch einige Besonderheiten, die sich ausschließlich in diesem Baustein wiederfinden. Der Baustein OPS.2.3 *Nutzung von Outsourcing* ist daher nicht auf Cloud-Dienste anzuwenden.

Die in diesem Baustein beschriebenen Gefährdungen und Anforderungen gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell.

Sicherheitsanforderungen, mit denen Anbietende ihre Cloud-Dienste schützen können, sind nicht Gegenstand dieses Bausteins. Gefährdungen und spezifische Sicherheitsanforderungen, die durch die Anbindung eines Cloud-

Dienstes über entsprechende Schnittstellen (englisch API, Application Programming Interface) als relevant anzusehen sind, werden ebenfalls nicht in diesem Baustein betrachtet.

Abgrenzung zum klassischen IT-Outsourcing

Beim Outsourcing werden Arbeits-, Produktions- oder Geschäftsprozesse einer Institution ganz oder teilweise zu externen Dienstleistenden ausgelagert. Dies ist ein etablierter Bestandteil heutiger Organisationsstrategien. Das klassische IT-Outsourcing ist meist so gestaltet, dass die komplette gemietete Infrastruktur exklusiv von einem Kunden oder einer Kundin genutzt wird (Single Tenant Architektur), auch wenn Anbietende von Outsourcing normalerweise mehrere Kunden oder Kundinnen haben. Zudem werden Outsourcing-Verträge meistens über längere Laufzeiten abgeschlossen.

Die Nutzung von Cloud-Diensten gleicht in vielen Punkten dem klassischen Outsourcing, aber es kommen noch einige Unterschiede hinzu, die zu berücksichtigen sind:

- Aus wirtschaftlichen Gründen teilen sich oft in einer Cloud mehrere Anwendende eine gemeinsame Infrastruktur.
- Cloud-Dienste sind dynamisch und dadurch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar. So können Cloud-basierte Angebote rascher an den tatsächlichen Bedarf der Anwendenden angepasst werden.
- Die in Anspruch genommenen Cloud-Dienste werden in der Regel mittels einer Webschnittstelle durch die Cloud-Anwendenden selbst gesteuert. So können sie automatisiert die genutzten Dienste auf ihre Bedürfnisse zuschneiden.
- Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen, die geographisch sowohl im In- als auch im Ausland weit verstreut sein können.
- Die Anwendenden können die genutzten Dienste und ihre Ressourcen einfach über Web-Oberflächen oder passende Schnittstellen administrieren, wobei wenig Interaktion mit den Cloud-Diensteanbietenden erforderlich ist.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.2.2 *Cloud-Nutzung* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Strategie für die Cloud-Nutzung

Cloud-Dienste in einer Institution einzusetzen, ist eine strategische Entscheidung. Durch eine fehlende oder unzureichende Strategie für die Cloud-Nutzung ist es z. B. möglich, dass sich eine Institution für ungeeignete Cloud-Dienste oder Cloud-Diensteanbietende entscheidet. Auch könnten die ausgewählten Cloud-Dienste mit der eigenen IT, den internen Geschäftsprozessen oder dem Schutzbedarf nicht kompatibel sein. Dies kann sich organisatorisch, technisch oder auch finanziell negativ auf die Geschäftsprozesse auswirken. Generell kann eine fehlende oder unzureichende Strategie für die Cloud-Nutzung dazu führen, dass die damit verbundenen Ziele nicht erreicht werden oder das Sicherheitsniveau signifikant sinkt.

2.2. Abhängigkeit von Cloud-Diensteanbietenden (Kontrollverlust)

Nutzt eine Institution externe Cloud-Dienste, ist sie mehr oder weniger stark von den Cloud-Diensteanbietenden abhängig. Dadurch kann es passieren, dass die Institution die ausgelagerten Geschäftsprozesse und die damit verbundenen Informationen nicht mehr vollständig kontrollieren kann, insbesondere deren Sicherheit. Auch ist die Institution trotz möglicher Kontrollen ab einem gewissen Punkt darauf angewiesen, dass die Cloud-Diensteanbietenden Sicherheitsmaßnahmen auch korrekt umsetzen. Machen sie das nicht, sind Geschäftsprozesse und geschäftskritische Informationen unzureichend geschützt.

Zudem kann die Nutzung externer Cloud-Dienste dazu führen, dass in der Institution Know-how über Informationssicherheit und -technik verloren geht. Dadurch kann die Institution unter Umständen gar nicht mehr beurteilen, ob die von Anbietenden ergriffenen Schutzmaßnahmen ausreichend sind. Auch ein Wechsel der Cloud-Dienstleistung ist so nur noch sehr schwer möglich. Die Cloud-Diensteanbietenden könnten diese Abhängigkeit zum Beispiel auch ausnutzen, um Preiserhöhungen durchzusetzen oder die Dienstleistungsqualität zu senken.

2.3. Mangelhaftes Anforderungsmanagement bei der Cloud-Nutzung

Wenn sich eine Institution dafür entscheidet, einen Cloud-Dienst zu nutzen, sind daran in der Regel viele Erwartungen geknüpft. So erhoffen sich Mitarbeitende beispielsweise eine höhere Leistungsfähigkeit oder einen größeren Funktionsumfang der ausgelagerten Dienste, während die Institutionsleitung auf geringere Kosten spekuliert. Ein mangelndes Anforderungsmanagement vor der Cloud-Nutzung kann jedoch dazu führen, dass die Erwartungen nicht erfüllt werden und der Dienst nicht den gewünschten Mehrwert, z. B. hinsichtlich der Verfügbarkeit, liefert.

2.4. Verstoß gegen rechtliche Vorgaben

Viele Anbietende bieten ihre Cloud-Dienste in einem internationalen Umfeld an. Damit unterliegen sie oft anderen nationalen Gesetzgebungen. Häufig sieht die Cloud-Kundschaft nur die mit dem Cloud Computing verbundenen Vorteile (z. B. Kostenvorteile) und schätzt die rechtlichen Rahmenbedingungen falsch ein, wie z. B. Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder Informationszugriff für Dritte. Dadurch könnten geltende Richtlinien und Vorgaben verletzt werden. Auch die Sicherheit der ausgelagerten Informationen könnte beeinträchtigt werden.

2.5. Fehlende Mandantenfähigkeit bei Cloud-Diensteanbietenden

Beim Cloud Computing teilen sich meistens verschiedene Institutionen eine gemeinsame Infrastruktur, wie z. B. IT-Systeme, Netze und Anwendungen. Werden beispielsweise die Ressourcen der verschiedenen Institutionen nicht ausreichend sicher voneinander getrennt, kann eine Institution eventuell auf die Bereiche einer anderen Institution zugreifen und dort Informationen manipulieren oder löschen.

2.6. Unzulängliche vertragliche Regelungen mit Cloud-Diensteanbietenden

Aufgrund von unzulänglichen vertraglichen Regelungen mit Cloud-Diensteanbietenden können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Verantwortungsbereiche, Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, kann es passieren, dass die Cloud-Diensteanbietenden unbeabsichtigt oder aufgrund fehlender Ressourcen Sicherheitsmaßnahmen nicht oder nur ungenügend umsetzen.

Auch wenn Situationen eintreten, die nicht eindeutig vertraglich geregelt sind, können Nachteile für die auftraggebende Institution daraus resultieren. So nutzen Cloud-Diensteanbietende für ihre Services häufig die Dienste Dritter. Bestehen hier unzureichende vertragliche Vereinbarungen oder wurden die Abhängigkeiten zwischen den Dienstleistenden und Dritten nicht offengelegt, kann sich dies auch negativ auf die Informationssicherheit und die Serviceleistung der Institution auswirken.

2.7. Mangelnde Planung der Migration zu Cloud-Diensten

Die Migration zu einem Cloud-Dienst ist fast immer eine kritische Phase. Durch mangelhafte Planungen können Fehler auftreten, die sich auf die Informationssicherheit innerhalb der Institution auswirken. Verzichtet eine Institution beispielsweise durch eine ungenügende Planungsphase leichtfertig auf eine stufenweise Migration, kann dies in der Praxis zu erheblichen Problemen führen. Gibt es im Vorfeld etwa keine Testphasen, Pilot-Benutzenden oder einen zeitlich begrenzten Parallelbetrieb von bestehender Infrastruktur und Cloud-Diensten, können wichtige Daten verloren gehen oder Dienste komplett ausfallen.

2.8. Unzureichende Einbindung von Cloud-Diensten in die eigene IT

Es ist erforderlich, dass Cloud-Dienste angemessen in die IT-Infrastruktur der Institution eingebunden werden. Setzen die Zuständigen dies nur unzureichend um, kann es passieren, dass die Benutzenden die beauftragten Cloud-Dienstleistungen nicht in vollem Umfang abrufen können. Die Cloud-Dienste liefern so eventuell nicht die erforderliche und vereinbarte Leistung oder auf sie kann gar nicht oder nur eingeschränkt zugegriffen werden. Dadurch können Geschäftsprozesse verlangsamt werden oder ganz ausfallen. Werden Cloud-Dienste falsch in die eigene IT eingebunden, können auch schwerwiegende Sicherheitslücken entstehen.

2.9. Unzureichende Regelungen für das Ende eines Cloud-Nutzungs-Vorhabens

Unzureichende Regelungen für eine mögliche Kündigung des Vertragsverhältnisses können gravierende Folgen für die Institution haben. Das ist erfahrungsgemäß immer dann besonders problematisch, wenn ein aus Sicht der Insti-

tution kritischer Fall unerwartet eintritt, wie beispielsweise die Insolvenz, der Verkauf der Cloud-Diensteanbietenden oder schwerwiegende Sicherheitsbedenken. Ohne eine ausreichende interne Vorsorge sowie genaue Vertragsregelungen kann sich die Institution nur schwer aus dem für die Cloud-Dienstleistung abgeschlossenen Vertrag lösen. In diesem Fall ist es schwierig bis unmöglich, den ausgelagerten Cloud-Dienst zeitnah beispielsweise auf eine andere Cloud-Computing-Plattform zu übertragen oder ihn wieder in die eigene Institution einzugliedern.

Auch kann eine unzureichend geregelte Datenlöschung nach Vertragsende dazu führen, dass unberechtigt auf die Informationen der Institution zugegriffen wird.

2.10. Unzureichendes Administrationsmodell für die Cloud-Nutzung

Werden Cloud-Dienste genutzt, verändert sich häufig das Rollenverständnis innerhalb des IT-Betriebs auf Seiten der nutzenden Institution. So entwickeln sich Administrierende oft weg von der klassischen Systemadministration hin zu Service-Administration. Wird dieser Prozess nicht ausreichend begleitet, kann sich dies negativ auf die Cloud-Nutzung auswirken, etwa, wenn die Administrierenden nicht das nötige Verständnis für die Umstellungen mitbringen oder sie für ihre neue Aufgabe nicht oder nur unzureichend geschult sind. In der Folge sind eventuell die Cloud-Dienste nicht ordnungsgemäß administriert und so nur noch eingeschränkt verfügbar oder sie fallen ganz aus.

2.11. Unzureichendes Notfallvorsorgekonzept

Eine unzureichende Notfallvorsorge hat bei der Cloud-Nutzung schnell gravierende Folgen. Wenn der Cloud-Dienst oder Teile hiervon ausfallen, führen Versäumnisse bei den Notfallvorsorgekonzepten bei Cloud-Diensteanbietenden sowie bei den Schnittstellen immer zu unnötig langen Ausfallzeiten mit entsprechenden Folgen für die Produktivität bzw. Dienstleistung der auftraggebenden Institution. Daneben können mangelhaft abgestimmte Notfallszenarien zwischen auftraggebender Institution und Dienstleistenden zu Lücken in der Notfallvorsorge führen.

2.12. Ausfall der IT-Systeme der Cloud-Diensteanbietenden

Bei Cloud-Diensteanbietenden können die dort betriebenen Prozesse, IT-Systeme und Anwendungen teilweise oder ganz ausfallen, wovon folglich auch die Cloud-Kundschaft betroffen ist. Werden die Institutionen unzureichend voneinander getrennt, kann auch ein ausgefallenes IT-System, das nicht der Institution zugeordnet ist, dazu führen, dass diese Institution ihre vertraglich zugesicherte Dienstleistung nicht mehr abrufen kann. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen Cloud-Diensteanbietenden und -Kundschaft ausfällt oder wenn die genutzte Cloud-Computing-Plattform erfolgreich angegriffen wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragte, Institutionsleitung, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung (B) [Fachverantwortliche, Institutionsleitung, Datenschutzbeauftragte]

Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele, Chancen und Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet. Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.

Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von Cloud-Diensteanbietenden bezogen werden sollen. Zudem MUSS sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für den geplanten Cloud-Dienst SOLLTE eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese SOLLTE wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte SOLLTE zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung (B) [Fachverantwortliche]

Auf Basis der Strategie für die Cloud-Nutzung MUSS eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellt werden. Sie MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Cloud-Dienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle Sicherheitsanforderungen an die Cloud-Diensteanbietenden sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste von internationalen Anbietenden genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

OPS.2.2.A3 Service-Definition für Cloud-Dienste (B) [Fachverantwortliche]

Für jeden Cloud-Dienst MUSS eine Service-Definition erarbeitet werden. Zudem SOLLTEN alle geplanten und genutzten Cloud-Dienste dokumentiert werden.

OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen (B) [Fachverantwortliche]

Basierend auf der Service-Definition für Cloud-Dienste MÜSSEN alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifiziert und dokumentiert werden. Es MUSS klar erkennbar sein, wie die Verantwortungsbereiche zwischen Cloud-Diensteanbietenden und der auftraggebenden Institution voneinander abgegrenzt sind.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst (S) [Fachverantwortliche]

Bevor zu einem Cloud-Dienst migriert wird, SOLLTE ein Migrationskonzept erstellt werden. Dafür SOLLTEN zunächst organisatorische Regelungen sowie die Aufgabenverteilung festgelegt werden. Zudem SOLLTEN bestehende Betriebsprozesse hinsichtlich der Cloud-Nutzung identifiziert und angepasst werden. Es SOLLTE sichergestellt werden, dass die eigene IT ausreichend im Migrationsprozess berücksichtigt wird. Auch SOLLTEN die Zuständigen ermitteln, ob die Mitarbeitenden auf Seiten der Institution zusätzlich geschult werden sollten.

OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten (S)

Bevor ein Cloud-Dienst genutzt wird, SOLLTE sorgfältig geplant werden, wie er in die IT der Institution eingebunden werden soll. Hierfür SOLLTE mindestens geprüft werden, ob Anpassungen der Schnittstellen, der Netzanbindung, des Administrationsmodells sowie des Datenmanagementmodells notwendig sind. Die Ergebnisse SOLLTEN dokumentiert und regelmäßig aktualisiert werden.

OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (S)

Auf Grundlage der identifizierten Sicherheitsanforderungen (siehe OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) SOLLTE ein Sicherheitskonzept für die Nutzung von Cloud-Diensten erstellt werden.

OPS.2.2.A8 Sorgfältige Auswahl von Cloud-Diensteanbietenden (S) [Institutionsleitung]

Basierend auf der Service-Definition für den Cloud-Dienst SOLLTE ein detailliertes Anforderungsprofil für Cloud-Diensteanbietende erstellt werden. Eine Leistungsbeschreibung und ein Lastenheft SOLLTEN erstellt werden. Für die Bewertung von Cloud-Diensteanbietenden SOLLTEN auch ergänzende Informationsquellen herangezogen werden. Ebenso SOLLTEN verfügbare Service-Beschreibungen der Cloud-Diensteanbietenden sorgfältig geprüft und hinterfragt werden.

OPS.2.2.A9 Vertragsgestaltung mit den Cloud-Diensteanbietenden (S) [Institutionsleitung]

Die vertraglichen Regelungen zwischen der auftraggebenden Institution und den Cloud-Diensteanbietenden SOLLTEN in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Informationen angepasst sein, die im Zusammenhang mit der Cloud-Nutzung stehen. Es SOLLTE geregelt werden, an welchem Standort die Cloud-Diensteanbietenden ihre Leistung erbringen. Zusätzlich SOLLTEN Eskalationsstufen und Kommunikationswege zwischen der Institution und den Cloud-Diensteanbietenden definiert werden. Auch SOLLTE vereinbart werden, wie die Daten der Institution sicher zu löschen sind. Ebenso SOLLTEN Kündigungsregelungen schriftlich fixiert werden. Die Cloud-Diensteanbietenden SOLLTEN alle Subunternehmen offenlegen, die sie für den Cloud-Dienst benötigen.

OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst (S) [Fachverantwortliche]

Die Migration zu einem Cloud-Dienst SOLLTE auf Basis des erstellten Migrationskonzeptes erfolgen. Während der Migration SOLLTE überprüft werden, ob das Sicherheitskonzept für die Cloud-Nutzung an potenzielle neue Anforderungen angepasst werden muss. Auch SOLLTEN alle Notfallvorsorgemaßnahmen vollständig und aktuell sein.

Die Migration zu einem Cloud-Dienst SOLLTE zunächst in einem Testlauf überprüft werden. Ist der Cloud-Dienst in den produktiven Betrieb übergegangen, SOLLTE abgeglichen werden, ob die Cloud-Diensteanbietenden die definierten Anforderungen der Institution erfüllen.

OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst (S)

Für die genutzten Cloud-Dienste SOLLTE ein Notfallkonzept erstellt werden. Es SOLLTE alle notwendigen Angaben zu Zuständigkeiten und Kontaktpersonen enthalten. Zudem SOLLTEN detaillierte Regelungen hinsichtlich der Datensicherung getroffen werden. Auch Vorgaben zu redundant auszulegenden Management-Tools und Schnittstellensystemen SOLLTEN festgehalten sein.

OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (S)

Alle für die eingesetzten Cloud-Dienste erstellten Dokumentationen und Richtlinien SOLLTEN regelmäßig aktualisiert werden. Es SOLLTE außerdem periodisch kontrolliert werden, ob die vertraglich zugesicherten Leistungen erbracht werden. Auch SOLLTEN sich die Cloud-Diensteanbietenden und die Institution nach Möglichkeit regelmäßig abstimmen. Ebenso SOLLTE geplant und geübt werden, wie auf Systemausfälle zu reagieren ist.

OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (S)

Die Institution SOLLTE sich von den Cloud-Diensteanbietenden regelmäßig nachweisen lassen, dass die vereinbarten Sicherheitsanforderungen erfüllt sind. Der Nachweis SOLLTE auf einem international anerkannten Regelwerk basieren (z. B. IT-Grundschutz, ISO/IEC 27001, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance). Die Institution SOLLTE prüfen, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzen Cloud-Diensteanbietende Subunternehmen, um die Cloud-Dienste zu erbringen, SOLLTEN Cloud-Diensteanbietende der Institution regelmäßig nachweisen, dass diese Subunternehmen die notwendigen Audits durchführen.

OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses (S) [Fachverantwortliche, Institutionsleitung]

Wenn das Dienstleistungsverhältnis mit den Cloud-Diensteanbietenden beendet wird, SOLLTE sichergestellt sein, dass dadurch die Geschäftstätigkeit oder die Fachaufgaben der Institution nicht beeinträchtigt wird. Die Verträge mit den Cloud-Diensteanbietenden SOLLTEN regeln, wie das jeweilige Dienstleistungsverhältnis geordnet aufgelöst werden kann.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.2.2.A15 Sicherstellung der Portabilität von Cloud-Diensten (H) [Fachverantwortliche]

Die Institution SOLLTE alle Anforderungen definieren, die es ermöglichen, Cloud-Diensteanbietende zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen. Zudem SOLLTE die Institution regelmäßig Portabilitätstests durchführen. In den Verträgen mit den Cloud-Diensteanbietenden SOLLTEN Vorgaben festgehalten werden, mit denen sich die notwendige Portabilität gewährleisten lässt.

OPS.2.2.A16 Durchführung eigener Datensicherungen (H) [Fachverantwortliche]

Die Institution SOLLTE prüfen, ob, zusätzlich zu den vertraglich festgelegten Datensicherungen der Cloud-Diensteanbietenden, eigene Datensicherungen erstellt werden sollen. Zudem SOLLTE sie detaillierte Anforderungen an einen Backup-Service erstellen.

OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung (H)

Wenn Daten durch Cloud-Diensteanbietende verschlüsselt werden, SOLLTE vertraglich geregelt werden, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen. Wenn eigene Verschlüsselungsmechanismen genutzt werden, SOLLTE ein geeignetes Schlüsselmanagement sichergestellt sein. Bei der Verschlüsselung SOLLTEN die eventuellen Besonderheiten des gewählten Cloud-Service-Modells berücksichtigt werden.

OPS.2.2.A18 Einsatz von Verbunddiensten (H) [Fachverantwortliche]

Es SOLLTE geprüft werden, ob bei einem Cloud-Nutzungs-Vorhaben Verbunddienste (Federation Services) eingesetzt werden.

Es SOLLTE sichergestellt sein, dass in einem SAML (Security Assertion Markup Language)-Ticket nur die erforderlichen Informationen an die Cloud-Diensteanbietenden übertragen werden. Die Berechtigungen SOLLTEN regelmäßig überprüft werden, sodass nur berechtigten Benutzenden ein SAML-Ticket ausgestellt wird.

OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitenden (H) [Personalabteilung]

Mit externen Cloud-Diensteanbietenden SOLLTE vertraglich vereinbart werden, dass in geeigneter Weise überprüft wird, ob das eingesetzte Personal qualifiziert und vertrauenswürdig ist. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI beschreibt in seiner Publikation „Anforderungskatalog Cloud Computing (C5)" Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten.

Die Cloud Security Alliance (CSA) gibt in ihrer Publikation „Security Guidance for Critical Areas of Focus in Cloud Computing" Empfehlungen zur Nutzung von Cloud-Diensten.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-144 „Guidelines on Security and Privacy in Public Cloud Computing" Empfehlungen zur Nutzung von Cloud-Diensten.

Die European Union Agency for Network and Information Security (ENISA) hat folgendes weiterführendes Dokument „Cloud Computing: Benefits, Risks and Recommendations for Information Security" zum Themenfeld Cloud Computing veröffentlicht.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security" in Kapitel SC 2 – Cloud Computing – Vorgaben zur Nutzung von Cloud-Diensten.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.2.3 Nutzung von Outsourcing

1. Beschreibung

1.1. Einleitung

Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietenden von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.

Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden kann. Typische Beispiele des klassischen „IT-Outsourcings", worauf sich dieser Baustein bezieht, sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe konkretisiert wird, wie Hosting, Housing oder Colocation.

Ein Outsourcing-Verhältnis betrifft neben den ursprünglichen Nutzenden und Anbietenden von Outsourcing in vielen Fällen weitere, den Anbietenden von Outsourcing nachgelagerte, Sub-Dienstleistende. Werden Teile von Geschäftsprozessen oder Tätigkeiten von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, so werden die von Nutzenden ausgelagerten Geschäftsprozesse oder Tätigkeiten weiter fragmentiert. Dies wirkt sich auf die Komplexität der Outsourcing-Kette aus, woraus eine schwindende Transparenz für die Nutzenden von Outsourcing folgt. Der Nachweis, dass die an die Anbietenden von Outsourcing gestellten Anforderungen erfüllt werden, erstreckt sich hierbei sowohl auf die Anbietenden von Outsourcing als auch auf die Sub-Dienstleistenden.

Zur besseren Verständlichkeit wird in diesem Baustein der Begriff „Prozess" stellvertretend für Geschäftsprozess, Tätigkeit oder Komponente verwendet, die ausgelagert wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Grundwerte der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit über den gesamten Lebenszyklus des Outsourcings durch die Nutzenden von Outsourcing sicherzustellen. Mit Outsourcing ist dabei das klassische „IT-Outsourcing" gemeint.

Die Anforderungen des Bausteins OPS.2.3 *Nutzung von Outsourcing* sollen dazu beitragen, dass potenzielle Gefährdungen für den Geschäftsbetrieb erkannt, vorgebeugt und vermindert werden. Risiken für eine Institution sollen hierdurch in einem für die Institution kontrollierbaren Rahmen bleiben. Dies kann durch mehr Transparenz und Steuerungsinstrumenten erreicht werden. Dazu wird die Institution in ihrer Planung, Durchführung und Kontrolle des Outsourcing-Prozesses über den gesamten Lebenszyklus hinsichtlich technischen und nicht-technischen Aspekten der Informationssicherheit unterstützt.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.2.3 *Nutzung von Outsourcing* ist für jede oder jeden Anbietenden von Outsourcing aus Sicht des Nutzenden von Outsourcing einmal anzuwenden.

Dieser Baustein behandelt Gefährdungen und Sicherheitsanforderungen aus Sicht der Nutzenden von Outsourcing-Leistungen und beschränkt sich auf die Anforderungen des Schutzes von Informationen seitens der auslagernden Institution.

Dieser Baustein behandelt nicht die Übertragungswege zu Anbietenden von Outsourcing.

Ebenso wird die Nutzung von Cloud-Diensten nicht in diesem Baustein behandelt, hierzu ist der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.

Vom klassischen „IT-Outsourcing" (wie dem Betrieb von Hard- und Software, Hosting, Housing usw.) abweichende Szenarien können mit dem Baustein OPS.2.3 *Nutzung von Outsourcing* mitunter nicht abschließend abgebildet werden und benötigen unter Umständen eine separate Risikoanalyse.

Als Sonderfall zählen Sicherheitsdienste, Reinigungskräfte, Wartungsdienste und Fremdpersonal, für die der Baustein OPS.2.3 *Nutzung von Outsourcing* nicht anzuwenden ist. Diese werden über die Anforderungen zu Sicherheitsdiensten, Reinigungskräften, Wartungsdiensten und Fremdpersonal in den Bausteinen ORP.1 *Organisation* und INF.1 *Allgemeines Gebäude* eingebunden.

Das Pendant zum Baustein OPS.2.3 *Nutzung von Outsourcing* bildet der Baustein OPS.3.2 *Anbieten von Outsourcing*, der das Outsourcing-Verhältnis aus der Sicht der Dienstleistenden behandelt. Zusammen bilden die beiden Bausteine ein ganzheitliches Bild des Outsourcing-Verhältnisses ab und sorgen mit ihren Anforderungen für ein grundlegendes sicheres Outsourcing-Vorhaben.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.2.3 *Nutzung von Outsourcing* von besonderer Bedeutung.

2.1. Unzureichende Strategie für das Outsourcing

Eine unzureichende Strategie führt dazu, dass die Informationssicherheit in Outsourcing-Vorhaben nicht angemessen berücksichtigt wird. Hierdurch wird die Informationssicherheit nicht angemessen in den einzelnen Phasen des Outsourcing-Lebenszyklus beachtet und somit kein ausreichendes Niveau der Informationssicherheit in der eigenen Institution sowie bei Anbietenden von Outsourcing angestrebt und umgesetzt. Dadurch können Prozesse beeinträchtigt, ausfallen und Informationen an unbefugte Dritte abfließen.

2.2. Gefahr des Outsourcings von institutionskritischen Prozessen

Prozesse, die aufgrund ihrer Kritikalität oder des Schutzbedarfs in der Institution verbleiben sollten, werden ausgelagert. Infolgedessen kann die Institution den Prozess, der für den ordentlichen Geschäftsbetrieb notwendig ist, nicht mehr angemessen kontrollieren und steuern. Wenn der Prozess ausfällt oder gestört wird, kann kein ordentlicher Geschäftsbetrieb sichergestellt werden. Darüber hinaus gewinnen die Anbietenden von Outsourcing einen größeren Einfluss. Es droht den Nutzenden von Outsourcing ein Steuerungsverlust.

2.3. Abhängigkeit von Anbietenden von Outsourcing

Entscheidet sich eine Institution für Outsourcing, macht sie sich damit auch von Anbietenden von Outsourcing abhängig. Mit dieser Abhängigkeit kann Wissen verloren gehen und die ausgelagerten Prozesse können nicht mehr vollständig kontrolliert werden. Außerdem könnte der Schutzbedarf der ausgelagerten Geschäftsprozesse und Informationen unterschiedlich eingeschätzt werden. Dies kann dazu führen, dass für den Schutzbedarf entsprechend ungeeignete Sicherheitsmaßnahmen umgesetzt werden. Häufig lagern Institutionen gesamte Geschäftsprozesse an Anbietende von Outsourcing aus. Die Anbietenden von Outsourcing können dadurch die Geschäftsprozesse mit schutzbedürftigen Informationen, Ressourcen und IT-Systemen vollständig kontrollieren. Gleichzeitig nimmt das Wissen über diese Bereiche bei Nutzenden von Outsourcing ab. Als Folge ist es möglich, dass die Nutzenden von Outsourcing Defizite der Informationssicherheit nicht mehr bemerken. Diese Situation könnte von Anbietenden von Outsourcing ausgenutzt werden, z. B. indem sie drastisch die Preise erhöhen oder die Qualität der Dienstleistungen abnimmt.

2.4. Unzureichendes Niveau der Informationssicherheit beim Outsourcing

Ein unzureichendes Niveau an Informationssicherheit kann dazu führen, dass die Informationssicherheit in Outsourcing-Vorhaben nicht angemessen berücksichtigt wird. Die Folge ist, dass die Anbietenden von Outsourcing keinen oder einen nur unzureichenden Standard der Informationssicherheit für den Outsourcing-Prozess aufrechterhalten. Folglich entstehen Schwachstellen, von denen IT-gestützte Angriffe sowie Datenverluste ausgehen können.

Darüber hinaus können für die Nutzenden von Outsourcing rechtliche Konsequenzen mit finanziellen Auswirkungen sowie Reputationsverluste entstehen.

2.5. Mangelhaftes Auslagerungsmanagement

Ein nicht vorhandenes oder nur teilweise umgesetztes Auslagerungsmanagement äußert sich dadurch, dass die laufenden ausgelagerten Prozesse unzureichend verwaltet werden. Dadurch verringert oder verliert sich die Transparenz über die ausgelagerten Prozesse. Hierdurch können Nutzende von Outsourcing die Anbietenden von Outsourcing nicht mehr kontrollieren und angemessen steuern. Die Nutzenden von Outsourcing können nicht mehr sicherstellen, dass die Anbietenden von Outsourcing in dem ausgelagerten Prozess die Informationssicherheit sorgfältig behandeln.

2.6. Unzulängliche vertragliche Regelungen mit Anbietenden von Outsourcing

Unzulängliche vertragliche Regelungen mit den Anbietenden von Outsourcing können zu Schwachstellen in der Informationssicherheit entlang des gesamten Outsourcing-Lebenszyklus führen. Die vertraglichen Regelungen definieren den gesamten Outsourcing-Prozess und stellen den Ausgangspunkt für Ansprüche der Nutzenden gegenüber den Anbietenden von Outsourcing dar. Aufgrund von unzulänglichen vertraglichen Regelungen mit den Anbietenden von Outsourcing können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, können möglicherweise aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden. Dies kann viele negative Auswirkungen nach sich ziehen, etwa, wenn regulatorische Anforderungen und Pflichten nicht erfüllt oder Auskunftspflichten und Gesetze nicht eingehalten werden. Wird bei der Vertragsgestaltung der Aspekt der Informationssicherheit nicht berücksichtigt, so können Prozesse und Daten der Nutzenden von Outsourcing unzureichend abgesichert werden.

2.7. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Je nach Outsourcing-Vorhaben kann es erforderlich sein, dass die Mitarbeitenden von Anbietenden von Outsourcing Zutritts-, Zugangs- und Zugriffsrechte zu IT-Systemen, Informationen, Gebäuden oder Räumen der Nutzenden von Outsourcing benötigen. Diese Rechte können ungeeignet vergeben, verwaltet und kontrolliert werden, hierdurch können im Extremfall sogar unautorisiert Rechte vergeben werden. Außerdem kann der notwendige Schutz der Informationen der Nutzenden von Outsourcing nicht mehr gewährleistet werden. Beispielsweise ist es ein gravierendes Sicherheitsrisiko, unkontrolliert administrative Berechtigungen an Mitarbeitende von Anbietenden von Outsourcing zu vergeben. Diese könnten Berechtigungen ausnutzen und sensible Informationen kopieren oder manipulieren.

2.8. Kontroll- und Steuerverlust durch Weiterverlagerungen

Teile von Geschäftsprozessen oder Tätigkeiten werden von Anbietenden von Outsourcing unter Umständen vollständig oder partiell an Sub-Dienstleistende weitergegeben. Da durch die zusätzlichen Beteiligten der Outsourcing-Prozess komplexer wird, wird dieser für die Nutzenden von Outsourcing intransparenter. Durch diese fehlende Transparenz können die Nutzenden von Outsourcing die ausgelagerten Prozesse nicht mehr angemessen kontrollieren und steuern. Darüber hinaus können Anbietende von Outsourcing versäumen, dass von Nutzenden von Outsourcing geforderte Mindestniveau der Informationssicherheit vom Sub-Dienstleistenden einzufordern. Eine Folge ist, dass unter Umständen die vereinbarten informationstechnischen Sicherheitsaspekte von den Sub-Dienstleistenden nicht vollständig umgesetzt werden.

2.9. Fehlende und unzulängliche Instrumente zur Steuerung von Anbietenden von Outsourcing

Damit eine Institution prüfen kann, ob die ausgelagerten Prozesse von Anbietenden von Outsourcing ordnungsgemäß umgesetzt werden, benötigt sie neben entsprechenden Vereinbarungen auch die Instrumente dazu. Dies können beispielsweise qualitative und quantitative Leistungskennzahlen (KPIs) sein. Um auf Minder- und Schlechtleistung reagieren zu können, werden entsprechend festgelegte Leistungskennzahlen benötigt. Fehlende und unzulängliche Instrumente führen dazu, dass die Anbietenden von Outsourcing nicht adäquat kontrolliert und gesteuert werden können. Dadurch kann nicht mehr geprüft und nachvollzogen werden, ob die festgelegten Sicherheitsanforderungen eingehalten werden.

2.10. Unzulängliche Regelungen für eine geplante und ungeplante Beendigung eines Outsourcing-Verhältnisses

Ein Outsourcing-Verhältnis kann ordentlich gekündigt oder auch außerordentlich beendet werden. Hierbei können unzulängliche oder fehlende Regelungen dazu führen, dass Hardware, Daten und Zugänge nicht oder nicht ordnungsgemäß an die Nutzenden von Outsourcing übergeben bzw. übermittelt werden.

2.11. Unzureichendes Notfallkonzept

Im Falle einer Störung, eines Notfalls oder einer Krise kann ein unzureichendes Notfallmanagement dazu führen, dass die ausgelagerten Prozesse ausfallen. Dabei bereitet insbesondere eine unzureichende Notfallvorsorge die Institution in ungenügendem Maße auf eine Not- oder Krisensituation vor. Eine effektive Notfallbewältigung kann auf dieser Grundlage nicht sichergestellt werden. Störungen, Not- und Krisensituationen können nicht kontrolliert werden und zu unmittelbaren wirtschaftlichen Auswirkungen führen. In diesem Fall ist nicht nur die eigene Institution, sondern auch alle angebundenen Institutionen, die in der Notfallvorsorge und Notfallbewältigung berücksichtigt werden müssen, betroffen. Kaskadeneffekte durch vor- und nachgelagerte Dienstleistende führen zu beträchtlichen Auswirkungen auf den Geschäftsbetrieb der Nutzenden von Outsourcing.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.2.3 *Nutzung von Outsourcing* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Beschaffungsstelle, Zentrale Verwaltung, Notfallbeauftragte, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.2.3.A1 Erstellung von Anforderungsprofilen für Prozesse (B) [Fachverantwortliche]

Falls keine Business-Impact-Analyse (BIA) vorhanden ist, MÜSSEN Anforderungsprofile in Form von Steckbriefen für die Prozesse angefertigt werden, die potenziell ausgelagert werden sollen. Diese Anforderungsprofile MÜSSEN die Funktion, verarbeite Daten, Schnittstellen sowie eine Bewertung der Informationssicherheit enthalten. Insbesondere MÜSSEN die Abhängigkeiten zwischen den Prozessen sowie zu untergeordneten Teilprozessen berücksichtigt werden. Die Anforderungsprofile MÜSSEN die Kritikalität des jeweiligen Prozesses für den ordentlichen Geschäftsbetrieb abbilden.

OPS.2.3.A2 Verfolgung eines risikoorientierten Ansatzes im Auslagerungsmanagement (B)

Für Prozesse, die potenziell ausgelagert werden sollen, MUSS risikoorientiert betrachtet und entschieden werden, ob diese ausgelagert werden können. Für diese Bewertung SOLLTEN die Anforderungsprofile als Grundlage genutzt werden. Wenn der Prozess ausgelagert wird, SOLLTE das Resultat im Auslagerungsregister abgelegt werden. Um Änderungen an Prozessen oder der Gefährdungslage zu berücksichtigen, MÜSSEN in regelmäßigen Abständen sowie anlassbezogen die ausgelagerten Prozesse erneut risikoorientiert betrachtet werden.

OPS.2.3.A3 Festlegung von Eignungsanforderungen an Anbietende von Outsourcing (B) [Fachverantwortliche, Institutionsleitung]

Interne Eignungsanforderungen an potenzielle Anbietende von Outsourcing MÜSSEN festgelegt werden. Diese Eignungsanforderungen MÜSSEN die erforderlichen Kompetenzen, um den Prozess aus Sicht der Informationssicherheit abzusichern, sowie die Reputation hinsichtlich der Vertrauenswürdigkeit und Zuverlässigkeit berücksichtigen. Diese Eignungsanforderungen SOLLTEN auf Basis der Unternehmensstrategie (siehe OPS.2.3.A8 *Erstellung einer Strategie für Outsourcing-Vorhaben*) erstellt werden. Es MUSS geprüft werden, ob potenzielle Interessenkonflikte vorliegen. Ferner SOLLTEN die Anbietenden von Outsourcing regelmäßig gegen die Eignungsanforderungen geprüft werden. Wenn die Anbietenden von Outsourcing nicht die Eignungsanforderungen erfüllen, SOLLTEN Handlungsmaßnahmen getroffen und in einem Maßnahmenkatalog festgehalten werden.

OPS.2.3.A4 Grundanforderungen an Verträge mit Anbietenden von Outsourcing (B)

Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. Diese Grundanforderungen MÜSSEN Aspekte der Informationssicherheit, einen Zustimmungsvorbehalt bei Weiterverlagerungen sowie ein Recht auf Prüfung, Revision und Audit beinhalten. Bei der Entwicklung der Grundanforderungen SOLLTEN die Resultate der risikoorientierten Betrachtung sowie Eignungsanforderungen an Anbietende von Outsourcing mit einfließen. Mit den Anbietenden von Outsourcing SOLLTE eine Verschwiegenheitserklärung zum Schutz von sensiblen Daten vereinbart werden. Die Grundanforderungen MÜSSEN in Vereinbarungen und Verträgen einheitlich umgesetzt werden. Auf Basis der Grundanforderungen SOLLTE eine einheitliche Vertragsvorlage erstellt und für alle Outsourcing-Vorhaben genutzt werden.

OPS.2.3.A5 Vereinbarung der Mandantenfähigkeit (B)

In einer Vereinbarung zur Mandantenfähigkeit mit den Anbietenden von Outsourcing MUSS sichergestellt werden, dass die Daten und Verarbeitungskontexte durch den Anbietenden von Outsourcing ausreichend sicher getrennt sind. In dieser Vereinbarung SOLLTE ein Mandantentrennungskonzept von den Anbietenden von Outsourcing gefordert werden. Das Mandantentrennungskonzept SOLLTE zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterscheiden und darlegen, mit welchen Mechanismen die Anbietenden von Outsourcing trennen.

OPS.2.3.A6 Festlegung von Sicherheitsanforderungen und Erstellung eines Sicherheitskonzeptes für das Outsourcing-Vorhaben (B)

Mit den Anbietenden von Outsourcing MUSS vertraglich vereinbart werden, dass IT-Grundschutz umgesetzt oder mindestens die Anforderungen aus den relevanten Bausteinen geeignet erfüllt werden. Darüber hinaus SOLLTE mit den Anbietenden von Outsourcing vereinbart werden, dass sie ein Managementsystem für Informationssicherheit (ISMS) etablieren. Die Nutzenden von Outsourcing MÜSSEN für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend auf den sich aus dem IT-Grundschutz ergebenen Sicherheitsanforderungen erstellen. Dabei MUSS das Sicherheitskonzept der Nutzenden mit den Anbietenden von Outsourcing abgestimmt werden. Ebenso SOLLTE jeder Anbietende ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Das Sicherheitskonzept der Anbietenden von Outsourcing und dessen Umsetzung SOLLTE zu einem gesamten Sicherheitskonzept zusammengeführt werden. Wenn Risikoanalysen notwendig sind, MÜSSEN Vereinbarungen getroffen werden, wie die Risikoanalyse geprüft und gegebenenfalls in das eigene Risikomanagement überführt werden kann. Die Nutzenden von Outsourcing oder unabhängige Dritte MÜSSEN regelmäßig überprüfen, ob das Sicherheitskonzept wirksam ist.

OPS.2.3.A7 Regelungen für eine geplante oder ungeplante Beendigung eines Outsourcing-Verhältnisses (B) [Fachverantwortliche, Institutionsleitung]

Für geplante sowie ungeplante Beendigungen des Outsourcing-Verhältnisses MÜSSEN Regelungen getroffen werden. Es MUSS festgelegt werden, wie alle Informationen, Daten und Hardware der Nutzenden vom Anbietenden von Outsourcing zurückgegeben werden. Hierbei MÜSSEN gesetzliche Vorgaben zur Aufbewahrung von Daten beachtet werden. Ferner SOLLTE überprüft werden, ob die Zugangs-, Zutritts- und Zugriffsrechte für die Anbietenden von Outsourcing mit der Beendigung des Outsourcing-Verhältnisses aufgehoben wurden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.2.3.A8 Erstellung einer Strategie für Outsourcing-Vorhaben (S) [Institutionsleitung]

Eine Strategie für Outsourcing-Vorhaben SOLLTE erstellt und etabliert werden. In dieser Strategie SOLLTEN die Ziele, Chancen und Risiken der Outsourcing-Vorhaben beschrieben werden. Die Strategie SOLL der Institution einen Rahmen für die Anforderungsprofile, Eignungsanforderung an Anbietende von Outsourcing sowie dem Auslagerungsmanagement vorgeben. Darüber hinaus SOLLTEN neben den wirtschaftlichen, technischen, organisatorischen und rechtlichen Rahmenbedingungen auch die relevanten Aspekte der Informationssicherheit berücksichtigt werden. Es SOLLTE eine Multi-Sourcing Strategie verfolgt werden, um Engpässe sowie Abhängigkeiten von Anbietenden von Outsourcing zu vermeiden. Die Nutzenden von Outsourcing SOLLTEN ausreichend Fähigkeiten, Kompetenzen sowie Ressourcen behalten, um einer Abhängigkeit gegenüber den Anbietenden von Outsourcing vorzubeugen.

OPS.2.3.A9 Etablierung einer Richtlinie zur Auslagerung (S) [Institutionsleitung]

Auf Basis der Strategie für Outsourcing-Vorhaben SOLLTE eine Richtlinie für den Bezug von Outsourcing-Dienstleistungen erstellt und in der Institution etabliert werden. Diese SOLLTE die allgemeinen Anforderungen basierend auf der Anforderung OPS.2.3.A4 *Grundanforderungen an Verträge mit Anbietenden von Outsourcing* sowie weitere Aspekte der Informationssicherheit für Outsourcing-Vorhaben standardisieren. Das Test- und Freigabeverfahren für Outsourcing-Vorhaben SOLLTE in dieser Richtlinie geregelt sein. Darüber hinaus SOLLTEN Maßnahmen berücksichtigt sein, um Compliance-Risiken bei Anbietenden von Outsourcing sowie bei Sub-Dienstleistenden zu bewältigen.

OPS.2.3.A10 Etablierung einer zuständigen Person für das Auslagerungsmanagement (S) [Personalabteilung]

Die verschiedenen Outsourcing-Vorhaben SOLLTEN durch eine zuständige Person für das Auslagerungsmanagement verwaltet werden. Die zuständige Person SOLLTE ernannt und die Befugnisse festgelegt und dokumentiert werden. Die zuständige Person SOLLTE als Schnittstelle in der Kommunikation zwischen den Nutzenden und Anbietenden von Outsourcing eingesetzt werden. Darüber hinaus SOLLTE die zuständige Person Berichte über das Outsourcing in regelmäßigen Abständen und anlassbezogen anfertigen und der Institutionsleitung übergeben. In der Vertragsgestaltung SOLLTE die zuständige Person einbezogen werden. Die zuständige Person SOLLTE ein angemessenes Kontingent von Arbeitstagen für die Aufgaben des Auslagerungsmanagements eingeräumt bekommen. Darüber hinaus SOLLTE die zuständige Person hinsichtlich Informationssicherheit geschult und sensibilisiert sein.

OPS.2.3.A11 Führung eines Auslagerungsregisters (S)

Die zuständige Person für das Auslagerungsmanagement SOLLTE ein Auslagerungsregister erstellen und pflegen, dass die Dokumentation der Outsourcing-Prozesse und Vorhaben in der Institution zentralisiert. Dieses SOLLTE auf der Basis der Anforderungsprofile erstellt werden und Informationen zu den Anbietenden von Outsourcing, Leistungskennzahlen, Kritikalität des Prozesses, abgeschlossenen Verträgen und Vereinbarungen sowie Änderungen enthalten. Änderungen am Auslagerungsregister SOLLTEN geeignet nachgehalten werden.

OPS.2.3.A12 Erstellung von Auslagerungsberichten (S)

Die zuständige Person für das Auslagerungsmanagement SOLLTE regelmäßig interne Auslagerungsberichte auf Basis des Auslagerungsregisters erstellen. Diese Auslagerungsberichte SOLLTEN den aktuellen Status des Outsourcing-Vorhabens mit allgemeinen Problemen und Risiken sowie Aspekte der Informationssicherheit enthalten. Der Auslagerungsbericht SOLLTE der Institutionsleitung vorgelegt werden.

OPS.2.3.A13 Bereitstellung der erforderlichen Kompetenzen bei der Vertragsgestaltung (S) [Institutionsleitung]

Die Verträge SOLLTEN durch verschiedene Vertreter aus unterschiedlichen Bereichen gestaltet werden. Dabei SOLLTE ein Interessenkonflikt zwischen operativem Geschäft und Informationssicherheit vermieden werden.

OPS.2.3.A14 Erweiterte Anforderungen an Verträge mit Anbietenden von Outsourcing (S)

Mit Anbietenden von Outsourcing SOLLTE vereinbart werden, auf welche Bereiche und Dienste die Anbietenden im Netz der Nutzenden von Outsourcing zugreifen dürfen. Der Umgang mit anfallenden Metadaten SOLLTE geregelt werden. Die Nutzenden SOLLTEN Leistungskennzahlen für die Anbietenden von Outsourcing definieren und

im Vertrag festlegen. Für den Fall, dass die vereinbarten Leistungskennzahlen unzureichend erfüllt werden, SOLLTEN mit den Anbietenden von Outsourcing Konsequenzen, wie z. B. Vertragsstrafen, festgelegt werden. Die Verträge SOLLTEN Kündigungsoptionen, um das Outsourcing-Verhältnisses aufzulösen, enthalten. Hierbei SOLLTE auch geregelt sein, wie das Eigentum der Nutzenden von Outsourcing zurückgegeben wird. Im Vertrag SOLLTEN Verantwortlichkeiten hinsichtlich des Notfall- und Krisenmanagements definiert und benannt werden.

OPS.2.3.A15 Anbindung an die Netze der Outsourcing-Partner (S)

Bevor das Datennetz der Nutzenden an das Datennetz der Anbietenden von Outsourcing angebunden wird, SOLLTEN alle sicherheitsrelevanten Aspekte schriftlich vereinbart werden. Es SOLLTE geprüft und dokumentiert werden, dass die Vereinbarungen für die Netzanbindung eingehalten werden. Das geforderte Sicherheitsniveau SOLLTE nachweislich bei den Anbietenden von Outsourcing umgesetzt und überprüft werden, bevor die Netzanbindung zu den Nutzenden von Outsourcing aktiviert wird. Bevor die Netze angebunden werden, SOLLTE mit Testdaten die Verbindung getestet werden. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.

OPS.2.3.A16 Prüfung der Anbietenden von Outsourcing (S)

Die Anbietenden von Outsourcing SOLLTEN hinsichtlich der vertraglich festgelegten Sicherheitsanforderungen überprüft und die Resultate dokumentiert werden. Die Anbietenden von Outsourcing sind in regelmäßigen Abständen und anlassbezogen zu auditieren.

OPS.2.3.A17 Regelungen für den Einsatz des Personals von Anbietenden von Outsourcing (S)

Die Beschäftigten der Anbietenden von Outsourcing SOLLTEN schriftlich verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die Regelungen der Nutzenden von Outsourcing einzuhalten. Die Beschäftigten der Anbietenden von Outsourcing SOLLTEN geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet werden. Für die Beschäftigten der Anbietenden von Outsourcing SOLLTEN Vertretungsregelungen existieren. Es SOLLTE ein geregeltes Verfahren festgelegt werden, das beschreibt, wie das Auftragsverhältnis mit den Beschäftigten der Anbietenden von Outsourcing beendet wird. Fremdpersonal der Anbietenden von Outsourcing, das kurzfristig oder nur einmal eingesetzt wird, SOLLTE wie Besuchende behandelt werden.

OPS.2.3.A18 Überprüfung der Vereinbarungen mit Anbietenden von Outsourcing (S)

Vereinbarungen mit Anbietenden von Outsourcing hinsichtlich der Angemessenheit der festgelegten Sicherheitsanforderungen sowie sonstigen Sicherheitsanforderungen SOLLTEN in regelmäßigen Abständen und anlassbezogen überprüft werden. Vereinbarungen mit Anbietenden von Outsourcing mit unzureichend festgelegten Sicherheitsanforderungen SOLLTEN nachgebessert werden. Die Anbietenden von Outsourcing SOLLTEN dazu verpflichtet werden, bei veränderter Gefährdungs- oder Gesetzeslage, die festgelegten Sicherheitsanforderungen nachzubessern.

OPS.2.3.A19 Überprüfung der Handlungsalternativen hinsichtlich einer geplanten oder ungeplanten Beendigung eines Outsourcing-Verhältnisses (S) [Beschaffungsstelle]

Handlungsalternativen SOLLTEN entwickelt werden für den Fall einer geplanten oder ungeplanten Beendigung des Outsourcing-Verhältnisses. Das Resultat SOLLTE in einem Maßnahmenkatalog für geplante und ungeplante Beendigung des Outsourcing-Verhältnisses dokumentiert werden. Dabei SOLLTEN auch alternative Anbietende von Outsourcing ermittelt werden, die über das notwendige Niveau an Informationssicherheit verfügen, um den Prozess sicher umzusetzen. Dies SOLLTE in regelmäßigen Abständen und anlassbezogen geprüft werden.

OPS.2.3.A20 Etablierung sowie Einbeziehung von Anbietenden von Outsourcing im Notfallkonzept (S) [Notfallbeauftragte]

Ein Notfallkonzept SOLLTE in der Institution etabliert sein. Dies SOLLTE auf einer Business-Impact-Analyse basieren und die Abhängigkeiten der ausgelagerten Prozesse mit den intern verbliebenen Prozessen berücksichtigen. Das Notfallkonzept SOLLTE den Anbietenden von Outsourcing in seiner Notfallvorsorge und -bewältigung berücksichtigen und mit diesem abgestimmt sein. Dabei SOLLTEN die Schnittstellen zu Anbietenden von Outsourcing mit Verantwortlichen benannt und besetzt werden, um einen Informationsaustausch sowie eine effektive Kollaboration in einer Not- oder Krisensituation zu ermöglichen. Gemeinsame Not- und Krisenfallpläne SOLLTEN für eine Störung

oder einen Ausfall der Anbietenden von Outsourcing erstellt werden. Standardisierte Protokolle und Berichte SOLLTEN zur Meldung von Sicherheitsvorfällen etabliert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.2.3.A21 Abschluss von ESCROW-Verträgen bei softwarenahen Dienstleistungen (H)

Wird Software von Anbietenden von Outsourcing bezogen, SOLLTE ein ESCROW-Vertrag abgeschlossen werden. Dieser SOLLTE Verwertungs- und Bearbeitungsrechte der Software sowie Herausgabefälle des Quellcodes regeln. Darüber hinaus SOLLTE festgelegt werden, wie häufig der Quellcode hinterlegt und dokumentiert wird. Weiterhin SOLLTEN Geheimhaltungspflichten über den hinterlegten Quellcode und die zugehörige Dokumentation geregelt werden.

OPS.2.3A22 Durchführung von gemeinsamen Notfall- und Krisenübungen (H) [Notfallbeauftragte]

Gemeinsame Notfall- und Krisenübungen mit den Anbietenden von Outsourcing SOLLTEN durchgeführt und dokumentiert werden (siehe DER.4 *Notfallmanagement*). Das Resultat der Übung SOLLTE dazu genutzt werden, um das Notfallkonzept sowie insbesondere die gemeinsamen Maßnahmenpläne zu verbessern. Die Notfall- und Krisenübungen SOLLTEN regelmäßig und anlassbezogen durchgeführt werden.

OPS.2.3.A23 Einsatz von Verschlüsselungen (H)

Sensible Daten SOLLTEN angemessen verschlüsselt werden, wenn sie zum Anbietenden von Outsourcing übertragen werden. Die abgelegten Daten SOLLTEN durch eine Datenverschlüsselung selbst oder des Speichermediums geschützt werden. Nach Möglichkeit SOLLTE eine vom BSI geprüfte und freigegebene Verschlüsselungssoftware genutzt werden.

OPS.2.3.A24 Sicherheits- und Eignungsüberprüfung von Mitarbeitenden (H) [Personalabteilung]

Mit externen Anbietenden von Outsourcing SOLLTE vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu SOLLTEN gemeinsam Kriterien festgelegt und dokumentiert werden.

OPS.2.3.A25 Errichtung und Nutzung einer Sandbox für eingehende Daten vom Anbietenden von Outsourcing (H)

Für eingehende Daten vom Anbietenden von Outsourcing SOLLTE eine Sandbox eingerichtet werden. Hierbei SOLLTEN E-Mail Anhänge in der Sandbox standardisiert geöffnet werden. Updates und Anwendungen eines softwarenahen Anbietenden von Outsourcing SOLLTEN in der Sandbox initial getestet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel A.15.2 „Steuerung der Dienstleistungserbringung von Lieferanten" Vorgaben für die Steuerung von Anbietenden von Outsourcing. In der DIN ISO 37500:2015-08 werden im „Leitfaden Outsourcing" weiterführende Informationen zum Umgang mit Anbietenden von Outsourcing aufgeführt.

Des Weiteren wird in der ISO 27002:2021 das Outsourcing-Verhältnis von Kapitel 5.19 bis 5.22 detailliert aufgeführt und spezifiziert somit die Vorgaben der ISO/IEC 27001:2013.

Das Information Security Forum (ISF) definiert in seinem Standard „The Standard of Good Practice for Information Security" verschiedene Anforderungen (SC1) an Anbietende von Outsourcing.

Der „Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland" des Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) liefert Informationen, wie Geschäftsprozesse an Anbietenden von Outsourcing ausgelagert werden können.

Ebenso hat die Bitkom den „Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis“ herausgegeben, die rechtlichen Aspekte von Outsourcing behandelt.

Das National Institute of Standards and Technology (NIST) nennt in der NIST Special Publication 800-53 Anforderungen an Anbietenden von Outsourcing.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.3.2 Anbieten von Outsourcing

1. Beschreibung

1.1. Einleitung

Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietende von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.

Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden kann. Typische Beispiele des klassischen „IT-Outsourcings", worauf sich dieser Baustein bezieht, sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe konkretisiert wird, wie Hosting, Housing oder Colocation.

Ein Outsourcing-Verhältnis betrifft neben den ursprünglichen Nutzenden und Anbietenden von Outsourcing in vielen Fällen weitere, den Anbietenden von Outsourcing nachgelagerte, Sub-Dienstleistende. Werden Teile von Geschäftsprozessen oder Tätigkeiten von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, so werden die von Nutzenden ausgelagerten Geschäftsprozesse oder Tätigkeiten weiter fragmentiert. Dies wirkt sich auf die Komplexität der Outsourcing-Kette aus, woraus eine schwindende Transparenz für die Nutzenden von Outsourcing folgt. Der Nachweis, dass die an die Anbietenden von Outsourcing gestellten Anforderungen erfüllt werden, erstreckt sich hierbei sowohl auf die Anbietenden von Outsourcing als auch auf die Sub-Dienstleistenden.

Zur besseren Verständlichkeit wird in diesem Baustein der Begriff „Prozess" stellvertretend für Geschäftsprozess, Tätigkeit oder Komponente verwendet, die ausgelagert wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Grundwerte der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit über den gesamten Lebenszyklus des Outsourcings durch die Anbietenden von Outsourcing sicherzustellen. Der Baustein soll dazu beitragen, dass die Anbietenden von Outsourcing gegenüber den Nutzenden von Outsourcing eine grundlegende Informationssicherheit gewährleistet. Mit Outsourcing ist dabei das klassische „IT-Outsourcing" gemeint.

Die Anforderungen des Bausteins OPS.3.2 *Anbieten von Outsourcing* sollen dazu beitragen, dass potenzielle Gefährdungen aus der Dienstleistung der Anbietenden von Outsourcing nicht die Nutzenden von Outsourcing gefährden. Dementsprechend sind diese Risiken zu mindern und vorzubeugen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.3.2 *Anbieten von Outsourcing* ist aus Sicht der Anbietenden auf jede oder jeden Nutzenden, der Dienstleistungen vom Anbietenden bezieht, einmal anzuwenden.

Dabei bezieht sich der Baustein auf die Perspektive der Anbietenden von Outsourcing im Outsourcing-Verhältnis. Die Anforderungen des Bausteins stellen sicher, dass fundamentale Sicherheitsstandards gegenüber den Nutzenden von Outsourcing eingehalten werden und dazu beitragen, dass die Anforderungen der Nutzenden von Outsourcing an die Informationssicherheit über den gesamten Outsourcing-Prozess eingehalten werden können.

Der Fall einer Weiterverlagerung wird in dem Baustein OPS.3.2 *Anbieten von Outsourcing* nur bedingt betrachtet, da dies ein weiteres Outsourcing-Verhältnis darstellt und somit die Anbietenden von Outsourcing den Baustein OPS.2.3 *Nutzung von Outsourcing* für diese Sub-Dienstleistenden modellieren müssen.

Vom klassischen „IT-Outsourcing" (wie dem Betrieb von Hard- und Software, Hosting, Housing usw.) abweichende Szenarien können mit dem Baustein OPS.3.2 *Anbieten von Outsourcing* mitunter nicht abschließend abgebildet werden und benötigen unter Umständen eine separate Risikoanalyse.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.3.2 *Anbieten von Outsourcing* von besonderer Bedeutung.

2.1. Unzureichendes Informationssicherheitsmanagement bei Anbietenden von Outsourcing

Ein mangelhaftes Informationssicherheitsmanagement kann dazu führen, dass die Schutzziele der Informationssicherheit durch die Anbietenden von Outsourcing nur unzureichend eingehalten werden. Durch einen Outsourcing-Vertrag sind die Anbietenden von Outsourcing dafür zuständig, das erforderliche Niveau an Informationssicherheit für den Outsourcing-Prozess einzuhalten. Sollten die Anbietenden von Outsourcing ihrer Zuständigkeit nicht nachkommen, so kann dies zu einer Gefahr für alle am Outsourcing-Prozess beteiligten Institutionen führen.

2.2. Unzureichendes Notfallmanagement der Anbietenden von Outsourcing

Wenn Störungen oder Notfälle bei Anbietenden von Outsourcing eintreten, kann dies zu einer Betriebsstörung führen, die auch die ausgelagerten Prozesse der Nutzenden von Outsourcing betreffen können und sich auf deren ordentlichen Geschäftsbetrieb auswirken. Insbesondere die Notfallvorsorge ist im Vorfeld von Not- und Krisensituation von entscheidender Bedeutung. Im Falle einer mangelhaften Notfallvorsorge kann für die Institution keine effektive Notfallbewältigung sichergestellt werden. Somit sind für die einzelnen Institutionen Störungen, Not- und Krisensituationen unter Umständen unkontrollierbar. Es kommt zu einem Kaskadeneffekt, der neben den Anbietenden von Outsourcing auch alle vor- und nachgelagerten Dienstleistenden sowie Kunden beeinträchtigt.

2.3. Unzulängliche vertragliche Regelungen mit Nutzenden von Outsourcing

Unzulänglichkeiten in der Vertragsgestaltung können dazu führen, dass die Informationssicherheit von ausgelagerten Prozessen der Nutzenden von Outsourcing unzureichend abgesichert ist. Vertragliche Regelungen definieren den gesamten Outsourcing-Prozess und stellen die rechtliche Grundlage für Ansprüche der Anbietenden von Outsourcing gegenüber den Nutzenden von Outsourcing dar. Somit übertragen sich die Unzulänglichkeiten aus der Vertragsgestaltung auf den gesamten Outsourcing-Lebenszyklus. Dies ist verbunden mit einer Vielzahl an möglichen Gefährdungsszenarien mit finanziellen und gesellschaftlichen Auswirkungen für die Nutzenden sowie Anbietenden von Outsourcing.

2.4. Schwachstellen bei der Anbindung Nutzender von Outsourcing

Die technische Anbindung der Nutzenden von Outsourcing an die Netze der Anbietenden von Outsourcing kann an den Schnittstellen zu technischen sowie organisatorischen Schwachstellen führen. Die technischen Schwachstellen in der Anbindung können zu Störungen, Datenverlust sowie zum Ausgangspunkt von IT-gestützte Angriffe führen. Dagegen können organisatorische Schwachstellen in Form von unbesetzten Schnittstellen zu Kommunikationsproblemen zwischen den Anbietenden und Nutzenden von Outsourcing führen. Diese können eine Gefahr für die Effizienz von Risikobewältigungsmaßnahmen in Not- und Krisensituationen darstellen.

2.5. Abhängigkeit von Sub-Dienstleistenden

Werden Tätigkeiten von Anbietenden von Outsourcing an Sub-Dienstleistende weiter verlagert, besteht das Risiko, dass die Sub-Dienstleistenden ihre Positionen ausnutzen, um Forderungen durchzusetzen sowie Vorgaben der Vereinbarung zu missachten. Es entsteht eine Abhängigkeit von Dritten, um die Kundenleistung zu erbringen. Sollten die Anbietenden von Outsourcing nicht in der Lage sein, eine Störung oder Ausfall der Sub-Dienstleistenden zu kompensieren, besteht eine zwingende Abhängigkeit. Dies bringt die Sub-Dienstleistenden gegenüber den Anbie-

tenden von Outsourcing in eine vorteilhafte Position. Die Sub-Dienstleistenden können davon absehen, die vertraglich geregelte Qualität sowie das festgelegte Niveau der Informationssicherheit einzuhalten. Dies beeinträchtigt das Outsourcing-Verhältnis mit den Nutzenden von Outsourcing und bedeutet für die Anbietenden von Outsourcing rechtliche und finanzielle Auswirkungen sowie einen Reputationsverlust.

2.6. Ungeeignete Konfiguration und Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Eine entweder ungeeignete oder unzureichende Konfiguration eines zentralen Verzeichnisdienstes kann dazu führen, dass Nutzende Rechte erhalten, die sie potenziell dazu befähigen auf sensible oder personenbezogene Daten der Anbietenden von Outsourcing oder anderer Kunden des Anbietenden von Outsourcing zuzugreifen. Unter Umständen erfordern Outsourcing-Vorhaben, dass Nutzende von Outsourcing auf den Informationsverbund der Anbietenden von Outsourcing zugreifen müssen. Dies ist mit entsprechenden Rechten für Zutritt, Zugang und Zugriff verbunden, die ein Risiko für die IT-Systeme, Informationen sowie Gebäude darstellen. Eine Folge ist, dass die Integrität und Vertraulichkeit dieser Daten gefährdet sind. Letztlich kann dies dazu führen, dass Vertragsstrafen von den Nutzenden von Outsourcing gegenüber den Anbietenden von Outsourcing geltend gemacht werden sowie ein Reputationsverlust für die Anbietenden von Outsourcing sowie ihre Kunden eintreten kann.

2.7. Unzureichende Mandantenfähigkeit bei Anbietenden von Outsourcing

Anbietende von Outsourcing haben in der Regel unterschiedliche Kunden, die auf die gleichen Ressourcen wie IT-Systeme, Netze oder Personal zurückgreifen. Sind IT-Systeme und Daten der Nutzenden von Outsourcing unzureichend voneinander getrennt und abgesichert, besteht die Gefahr, dass Nutzende auf die Bereiche anderer Nutzender zugreifen und unberechtigt auf Daten zugreifen können. Dies stellt einen unmittelbaren Verstoß gegen die Vertraulichkeit der jeweiligen Daten der Nutzenden dar. Insbesondere ist dies problematisch bei Nutzenden von Outsourcing, die im Wettbewerb miteinander stehen. Die Auswirkungen wären Reputationsverlust für die Anbietenden von Outsourcing sowie rechtliche Folgen durch die geschädigten Nutzenden von Outsourcing.

2.8. Kontroll- und Steuerungsverlust bei der Weiterverlagerung an Sub-Dienstleistende

Ausgelagerte Prozesse werden von Anbietenden von Outsourcing unter Umständen im Rahmen einer Weiterverlagerung vollständig oder partiell an Sub-Dienstleistende weitergegeben. Eine unzureichende Kontrolle der Sub-Dienstleistenden führt dazu, dass vereinbarte Aspekte der Informationssicherheit von Sub-Dienstleistenden unzureichend eingehalten werden. Dies hat im weiteren Verlauf Konsequenzen für das Outsourcing-Verhältnis mit den Nutzenden von Outsourcing sowie unmittelbare finanzielle Auswirkungen und Reputationsverluste für die Anbietenden von Outsourcing zur Folge.

2.9. Unzulängliche Regelungen für eine geplante oder ungeplante Beendigung eines Outsourcing-Verhältnisses

Unzulängliche Regelungen für das Ende eines Outsourcing-Verhältnisses können dazu führen, dass Hardware sowie Daten abschließend nicht ordnungsgemäß an die Nutzenden von Outsourcing übergeben oder übermittelt werden. Hinzu kommt, dass vorhandene Kundendaten nicht nach Speicherfrist der einschlägigen Gesetze und Vorschriften ordnungsgemäß gelöscht werden. Ein Outsourcing-Verhältnis kann durch eine ordentliche Kündigung sowie durch außerordentliche Gründe beendet werden. Exemplarisch hierfür ist eine Insolvenz von Anbietenden von Outsourcing. Die Anbietenden von Outsourcing schützen unter Umständen nach der Vertragsauflösung die vorhandenen Daten der Nutzenden von Outsourcing nicht angemessen gemäß des Schutzbedarfs des jeweiligen Eigentümers. Die Daten können in die Hand Dritter gelangen und bei Veröffentlichung zu Reputationsverlust führen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.3.2 *Anbieten von Outsourcing* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Institution, Datenschutzbeauftragte, Notfallbeauftragte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.3.2.A1 Einhaltung der Schutzziele der Informationssicherheit durch ein Informationssicherheitsmanagement (B)

Der Schutzbedarf für Vertraulichkeit, Integrität und Verfügbarkeit von Nutzenden von Outsourcing MUSS im Outsourcing-Prozess berücksichtigen werden. Dabei MUSS sichergestellt werden, dass das von den Nutzenden von Outsourcing geforderte Minimum an Informationssicherheit eingehalten wird. Zudem MÜSSEN die geltenden regulatorischen und gesetzlichen Aspekte berücksichtigt werden.

OPS.3.2.A2 Grundanforderungen an Verträge mit Nutzenden von Outsourcing (B)

Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. Diese SOLLTEN einheitlich in Verträgen umgesetzt werden. Diese Grundanforderungen MÜSSEN Aspekte der Informationssicherheit und Sicherheitsanforderungen der Nutzenden von Outsourcing beinhalten. Zudem MÜSSEN sie beinhalten, wie mit Weiterverlagerungen durch die Anbietenden umgegangen wird. Die Grundanforderungen MÜSSEN beinhalten, dass die Nutzenden das Recht haben Prüfungen, Revisionen und Auditierungen durchzuführen, um sicherzustellen, dass die vertraglich geregelten Anforderungen an die Informationssicherheit eingehalten werden. Mit den Nutzenden von Outsourcing SOLLTE eine Verschwiegenheitserklärung zum Schutz von sensiblen Daten, Vereinbarungen zum Informationsaustausch und Service-Level-Agreements vereinbart werden. Die Grundanforderungen MÜSSEN in Vereinbarungen und Verträgen einheitlich umgesetzt werden. Auf Basis der Grundanforderungen SOLLTE eine einheitliche Vertragsvorlage erstellt und für alle Outsourcing-Vorhaben genutzt werden.

OPS.3.2.A3 Weitergabe der vertraglich geregelten Bestimmungen mit Nutzenden von Outsourcing an Sub-Dienstleistende (B)

Werden Prozesse von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, MÜSSEN die vertraglichen Bestimmungen mit den Nutzenden von Outsourcing an die Sub-Dienstleistenden weitergegeben werden. Dies MUSS in den Verträgen mit den Sub-Dienstleistenden entsprechend festlegt und durchgesetzt werden. Auf Nachfrage von Nutzenden von Outsourcing MÜSSEN diese Verträge vorgelegt werden.

OPS.3.2.A4 Erstellung eines Mandantentrennungskonzepts (B)

Es MUSS ein Mandantentrennungskonzept erstellt und umgesetzt werden. Das Mandantentrennungskonzept MUSS sicherstellen, dass Daten und Verarbeitungskontexte verschiedener Nutzender von Outsourcing ausreichend sicher getrennt werden. Dabei MUSS zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterschieden werden. Es MUSS dargelegt werden, mit welchen Mechanismen die Anbietenden von Outsourcing die Mandanten trennen. Die benötigten Mechanismen zur Mandantentrennung MÜSSEN durch die Anbietenden von Outsourcing ausreichend umgesetzt werden. Das Mandantentrennungskonzept MUSS durch die Anbietenden von Outsourcing erstellt und den Nutzenden von Outsourcing zur Verfügung gestellt werden. Darüber hinaus MUSS es für den Schutzbedarf der Daten der Nutzenden von Outsourcing eine angemessene Sicherheit bieten.

OPS.3.2.A5 Erstellung eines Sicherheitskonzepts für die Outsourcing-Dienstleistung (B)

Die Anbietenden von Outsourcing MÜSSEN für ihre Dienstleistungen ein Sicherheitskonzept erstellen. Für individuelle Outsourcing-Vorhaben MÜSSEN zusätzlich spezifische Sicherheitskonzepte erstellt werden, die auf den Sicherheitsanforderungen der Nutzenden von Outsourcing basieren. Das Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben SOLLTE jedem und jeder Nutzenden von Outsourcing vorgelegt werden. Das Sicherheitskonzept der

Anbietenden von Outsourcing und dessen Umsetzung SOLLTE zu einem gesamten Sicherheitskonzept zusammengeführt werden. Anbietende und Nutzende von Outsourcing MÜSSEN gemeinsam Sicherheitsziele erarbeiten und diese dokumentieren. Es MUSS außerdem eine gemeinsame Klassifikation für alle schutzbedürftigen Informationen erstellt werden. Darüber hinaus MÜSSEN die Anbietenden von Outsourcing regelmäßig überprüfen, ob das Sicherheitskonzept umgesetzt wurde.

OPS.3.2.A6 Regelungen für eine geplante und ungeplante Beendigung eines Outsourcing-Verhältnisses (B)

Es MÜSSEN Regelungen getroffen werden, wie verfahren wird, wenn Outsourcing-Verhältnisse geplant oder ungeplant beendet werden. Es MUSS festgelegt werden, wie alle Informationen, Daten und Hardware der Nutzenden von den Anbietenden von Outsourcing zurückgegeben werden. Anschließend MÜSSEN die verbleibenden Datenbestände der Nutzenden von Outsourcing nach Ablauf der gesetzlichen Vorgaben zur Datenaufbewahrung sicher gelöscht werden. Dies MUSS durch die Anbietenden von Outsourcing dokumentiert werden. Ferner SOLLTE überprüft werden, ob die Zugangs-, Zutritts- und Zugriffsrechte für die Nutzenden von Outsourcing aufgehoben wurden, nachdem das Outsourcing-Verhältnis beendet wurde.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.3.2.A7 Bereitstellung der ausgelagerten Dienstleistung durch multiple Sub-Dienstleistende (S)

Werden Prozesse von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, SOLLTEN die Anbietenden von Outsourcing mehrere qualifizierte Sub-Dienstleistende zur Verfügung haben, falls Sub-Dienstleistende ausfallen oder kündigen. Dies SOLLTE gemeinsam mit den Nutzenden von Outsourcing dokumentiert werden.

OPS.3.2.A8 Erstellung einer Richtlinie für die Outsourcing-Dienstleistungen (S)

Es SOLLTE eine Richtlinie für das Anbieten von Outsourcing-Dienstleistungen erstellt und in der Institution etabliert werden. Diese SOLLTE das Test- und Freigabeverfahren regeln. Dabei SOLLTE die Weiterverlagerung an Sub-Dienstleistende berücksichtigt werden. Die Richtlinie SOLLTE Maßnahmen berücksichtigen, um Compliance-Risiken bei Anbietenden von Outsourcing sowie bei Sub-Dienstleistenden zu bewältigen.

OPS.3.2.A9 Überprüfung der Vereinbarung mit Nutzenden von Outsourcing (S)

Vereinbarungen mit Nutzenden von Outsourcing hinsichtlich der Angemessenheit der festgelegten Sicherheitsanforderungen sowie sonstigen Sicherheitsanforderungen SOLLTEN in regelmäßigen Abständen und anlassbezogen überprüft werden. Vereinbarungen mit Nutzenden von Outsourcing mit unzureichend festgelegten Sicherheitsanforderungen SOLLTEN nachgebessert werden. Bei veränderter Gefährdungs- oder Gesetzeslage SOLLTEN die festgelegten Sicherheitsanforderungen nachgebessert werden. Alle Änderungen SOLLTEN durch die Anbietenden von Outsourcing dokumentiert werden.

OPS.3.2.A10 Etablierung eines sicheren Kommunikationskanals und Festlegung der Kommunikationspartner (S)

Die Anbietenden von Outsourcing SOLLTEN einen sicheren Kommunikationskanal zu den Nutzenden von Outsourcing einrichten. Es SOLLTE dokumentiert sein, welche Informationen über diesen Kommunikationskanal an den Outsourcing-Partner übermittelt werden. Dabei SOLLTE sichergestellt werden, dass an den jeweiligen Enden des Kommunikationskanals entsprechend Zuständige benannt sind. Dabei SOLLTE regelmäßig und anlassbezogen überprüft werden, ob diese Personen noch in ihrer Funktion als dedizierte Kommunikationspartner beschäftigt sind. Zwischen den Outsourcing-Partnern SOLLTE geregelt sein, nach welchen Kriterien welcher Kommunikationspartner welche Informationen erhalten darf.

OPS.3.2.A11 Etablierung eines Notfallkonzepts (S) [Notfallbeauftragte]

Ein Notfallkonzept SOLLTE in der Institution etabliert sein. In diesem Notfallkonzept SOLLTEN Nutzende von Outsourcing sowie Sub-Dienstleistende berücksichtigt werden.

OPS.3.2.A12 Durchführung einer risikoorientierten Betrachtung von Prozessen, Anwendungen und IT-Systemen (S)

Werden Prozesse, Anwendungen oder IT-Systeme neu aufgebaut und Kunden bereitgestellt, SOLLTEN diese regelmäßig und anlassbezogen risikoorientiert betrachtet und dokumentiert werden. Aus den sich daraus ergebenen Ergebnissen SOLLTEN geeignete Maßnahmen festgelegt werden. Darüber hinaus SOLLTEN die Resultate dazu verwendet werden, um das Informationssicherheitsmanagement weiter zu verbessern.

OPS.3.2.A13 Anbindung an die Netze der Outsourcing-Partner (S)

Bevor das Datennetz der Anbietenden an das Datennetz der Nutzenden von Outsourcing angebunden wird, SOLLTEN alle sicherheitsrelevanten Aspekte schriftlich vereinbart werden. Bevor beide Netze verbunden werden, SOLLTEN sie auf bekannte Sicherheitslücken analysiert werden. Es SOLLTE geprüft werden, ob die Vereinbarungen für die Netzanbindung eingehalten werden und das geforderte Sicherheitsniveau nachweislich erreicht wird. Bevor die Netze angebunden werden, SOLLTE mit Testdaten die Verbindung getestet werden. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.

OPS.3.2.A14 Überwachung der Prozesse, Anwendungen und IT-Systeme (S)

Die für Kunden eingesetzten Prozesse, Anwendungen und IT-Systeme SOLLTEN kontinuierlich überwacht werden.

OPS.3.2.A15 Berichterstattung gegenüber den Nutzenden von Outsourcing (S)

Die Anbietenden von Outsourcing SOLLTEN den Nutzenden von Outsourcing in festgelegten Abständen Berichte über den ausgelagerten Prozess bereitstellen. Es SOLLTE ein Bericht an die Nutzenden von Outsourcing versendet werden, wenn Änderungen am Prozess durch die Anbietenden von Outsourcing oder Sub-Dienstleistenden stattfanden. Dazu SOLLTEN standardisierte Protokolle zur Berichterstattung etabliert werden.

OPS.3.2.A16 Transparenz über die Outsourcing-Kette der ausgelagerten Kundenprozesse (S)

Die Anbietenden von Outsourcing SOLLTEN ein Auslagerungsregister für die in Kundenprozessen eingesetzten Sub-Dienstleistenden führen. Dieses SOLLTE Informationen zu den Sub-Dienstleistenden, Leistungskennzahlen, Kritikalität der Prozesse, abgeschlossenen Verträgen und Vereinbarung sowie Änderungen enthalten. Änderungen am Auslagerungsregister SOLLTEN nachgehalten werden. Das Auslagerungsregister SOLLTE auch die Weiterverlagerungen durch die Sub-Dienstleistenden behandeln. Die Anbietenden von Outsourcing SOLLTEN das Auslagerungsregister regelmäßig und anlassbezogen überprüfen.

OPS.3.2.A17 Zutritts-, Zugangs- und Zugriffskontrolle (S)

Zutritts-, Zugangs- und Zugriffsberechtigungen SOLLTEN sowohl für das Personal der Anbietenden von Outsourcing als auch für das Personal der Nutzenden von Outsourcing geregelt sein. Ebenfalls SOLLTEN Zutritts-, Zugangs- und Zugriffsberechtigungen für Auditoren und andere Prüfer festgelegt werden. Dabei SOLLTEN nur so viele Rechte vergeben werden, wie für die Tätigkeit notwendig ist.

OPS.3.2.A18 Regelungen für den Einsatz von Sub-Dienstleistenden (S)

Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden SOLLTEN in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit der Anbietenden von Outsourcing unterrichtet werden. Soweit es gefordert ist, SOLLTEN das Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden nach Vorgaben der Nutzenden von Outsourcing überprüft werden, z. B. durch ein Führungszeugnis. Das Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden SOLLTEN schriftlich dazu verpflichtet werden, einschlägige Gesetze und Vorschriften, Vertraulichkeitsvereinbarungen sowie interne Regelungen einzuhalten. Es SOLLTEN Vertretungsregelungen in allen Bereichen existieren.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.